

UNCLASSIFIED



NORTH DAKOTA HOMELAND SECURITY ANTI-TERRORISM SUMMARY



The North Dakota Open Source Anti-Terrorism Summary is a product of the North Dakota State and Local Intelligence Center (NDSLIC). It provides open source news articles and information on terrorism, crime, and potential destructive or damaging acts of nature or unintentional acts. Articles are placed in the Anti-Terrorism Summary to provide situational awareness for local law enforcement, first responders, government officials, and private/public infrastructure owners.

UNCLASSIFIED

UNCLASSIFIED

NDSLIC DISCLAIMER

The Anti-Terrorism Summary is a non-commercial publication intended to educate and inform. Further reproduction or redistribution is subject to original copyright restrictions. NDSLIC provides no warranty of ownership of the copyright, or accuracy with respect to the original source material.

QUICK LINKS

[North Dakota](#)

[Energy](#)

[Regional](#)

[Food and Agriculture](#)

[National](#)

[Government Sector \(including
Schools and Universities\)](#)

[International](#)

[Information Technology and
Telecommunications](#)

[Banking and Finance Industry](#)

[Chemical and Hazardous Materials
Sector](#)

[National Monuments and Icons](#)

[Commercial Facilities](#)

[Postal and Shipping](#)

[Communications Sector](#)

[Public Health](#)

[Critical Manufacturing](#)

[Transportation](#)

[Defense Industrial Base Sector](#)

[Water and Dams](#)

[Emergency Services](#)

[North Dakota Homeland Security
Contacts](#)

UNCLASSIFIED

NORTH DAKOTA

Nothing Significant to Report

REGIONAL

Nothing Significant to Report

NATIONAL

Refer to *Energy* section; item # 1 for related information.

INTERNATIONAL

Refer to *Banking and Finance Industry* section; item # 3 for related information.

BANKING AND FINANCE INDUSTRY

Feds: 9 sold worthless stocks in massive scheme. Federal authorities charged nine individuals with running a 'pump and dump' penny stocks scheme that defrauded investors around the world of more than \$140 million. Source: http://www.cbsnews.com/8301-505123_162-57598360/feds-9-sold-worthless-stocks-in-massive-scheme/

Payment processing computer systems of smartphone experts hacked. An online smartphone accessories retailer notified customers of a data breach that gave hackers access to Smartphone Experts' customer personal information and credit and debit card information. The breach, identified July 12 began April 25, 2012. The information stored on the impacted computer was encrypted, but hackers can still access the decryption feature of the system to access the information. Source: <http://news.softpedia.com/news/Payment-Processing-Computer-Systems-of-Smartphone-Experts-Hacked-375035.shtml>

Hacker pleads not guilty to stealing 160M credit cards. A man accused of participating in the biggest hacking scheme in U.S. history spanning from 2005 to 2012 pleaded not guilty August 12 to stealing more than 160 million credit card numbers by hacking into corporations and selling the stolen credit card information to other parties. The Russian national and several others cost the companies and customers a combined total of more than \$300 million. Source: http://news.cnet.com/8301-1009_3-57598232-83/hacker-pleads-not-guilty-to-stealing-160m-credit-cards/

CHEMICAL AND HAZARDOUS MATERIALS SECTOR

Refer to *Energy* section; item # 2 for related information.

COMMERCIAL FACILITIES

Nothing Significant to Report

COMMUNICATIONS SECTOR

Nothing Significant to Report

CRITICAL MANUFACTURING

Philips Lighting recalls Endura and Ambient LED bulbs due to shock hazard. Philips Lighting announced a recall of about 99,000 Endura and Ambient LED light bulbs due to a lead wire in the bulb having an improper fitting which can electrify the lamp and create a shock hazard.

Source: <https://www.cpsc.gov/en/Recalls/2013/Philips-Lighting-Recalls-Endura-and-Ambient-LED-Bulbs/>

Hyundai recalls 23K Santa Fe SUVs; can lose power. Hyundai announced a recall of about 23,000 model year 2013 Santa Fe vehicles in the U.S. and Canada due to a right axle shaft that can fail, causing a loss of power while in motion or a rollaway hazard if parked. Source: http://www.philly.com/philly/business/consumer_news/20130813_ap_9da1adb9ec1f4a12b2cf1ce53721394a.html

DEFENSE/ INDUSTRY BASE SECTOR

Northrop Grumman hacked, linguists program database compromised. A Northrop Grumman company database containing the personal information of individuals who have applied to or were retained as linguists for the company's Balkans Linguist Support Program was accessed by hackers. The affected database, which has been taken offline, contained names, dates of birth, blood types, Social Security numbers, contact information, and other government-issued identification numbers. Source: <http://news.softpedia.com/news/Northrop-Grumman-Hacked-Linguists-Program-Database-Compromised-376000.shtml>

EMERGENCY SERVICES

(Colorado) Guns and armor stolen from two unmarked police cars in Aurora. Two rifles, a pistol, and a ballistic vest were stolen August 14 from a pair of unmarked Adams County Sheriff's Office vehicles parked in southeast Aurora. The Aurora Police Department is investigating. Source: <http://kdvr.com/2013/08/15/guns-and-armor-stolen-from-two-unmarked-police-cars-in-aurora/>

Massachusetts man charged with making hoax emergency services calls to elicit SWAT team response. The FBI arrested and charged a Massachusetts man for making several fake calls to numerous police departments around the U.S. in order to elicit an armed police response for the purpose of harassing his intended swatting victim. The suspect agreed to plead guilty after

UNCLASSIFIED

making multiple threats to using firearms and explosives while placing his calls. Source: <http://www.fbi.gov/boston/press-releases/2013/massachusetts-man-charged-with-making-hoax-emergency-services-calls-to-elicite-swat-team-response>

ENERGY

U.S. electricity grid 'highly vulnerable' to blackouts, report says. A report issued August 12 by the White House and the U.S. Energy Department stated the U.S. electricity grid is extremely vulnerable to blackouts due to extreme weather events fueled by climate change. The aging of the grid has made the public more susceptible to outages caused by severe weather. Source: <http://www.baltimoresun.com/business/bs-bz-electricity-grid-20130812,0,4769274.story>

(Illinois) Gas pipeline fire in western Illinois sends flames hundreds of feet into the sky; no injuries. Crews were able to gain control of a fire that ignited after a fuel pipeline beneath a western Illinois cornfield exploded August 12 and forced the evacuation of dozens of residents. Evacuees were allowed to return by August 13. Source: http://www.washingtonpost.com/business/gas-pipeline-fire-in-western-illinois-sends-flames-hundreds-of-feet-into-the-sky-no-injuries/2013/08/13/b5ba0b36-040b-11e3-bfc5-406b928603b2_story.html

FOOD AND AGRICULTURE

Salmonella outbreak sickens 307 in 37 states. Officials reported August 9 that a major multistate outbreak of Salmonella Typhimurium linked to baby poultry, has sickened more than 300 people in 37 States in a six month period. Source: <http://consumer.healthday.com/infectious-disease-information-21/misc-infections-news-411/salmonella-outbreak-sickens-307-in-37-states-679131.html>

Cyclospora infections rise to 514. According to the U.S. Centers for Disease Control and Prevention at least 514 people were found ill from Cyclospora infections since June across 17 States, including 30 individuals who were hospitalized. Source: <http://www.foodsafetynews.com/2013/08/cyclospora-infections-rise-to-514/>

GOVERNMENT SECTOR (INCLUDING SCHOOLS AND UNIVERSITIES)

(California) Copper theft severs state websites. At least eight State of California departments lost access to their Web sites and email August 14 after thieves stole part of a fiber and copper line that runs between Vacaville and Napa. Source: <http://www.latimes.com/local/political/la-me-pc-copper-theft-california-websites-20130815,0,5792405.story>

(Texas) Student arrested for hacking into Denton High School's system. Authorities arrested a student of Denton High School in Texas after he hacked into the school's Wi-Fi system in March

UNCLASSIFIED

UNCLASSIFIED

and April and used school printers to print out stolen security codes and test results. The student was retaliating against the school after a teacher refused to grade a report he wrote. Source: <http://news.softpedia.com/news/Student-Arrested-for-Hacking-into-Denton-High-School-s-Systems-374869.shtml>

INFORMATION TECHNOLOGY AND TELECOMMUNICATIONS

Zeus variant uses infected systems to check for availability of Instagram usernames.

Researchers at RSA discovered a variant of the Zeus malware that infects computers and can then run search engine queries, check the availability of Instagram account names for use in selling fake followers, and automatically 'like' photos on Instagram. Source: <http://news.softpedia.com/news/ZeuS-Variant-Uses-Infected-Systems-to-Check-for-Availability-of-Instagram-Usernames-375775.shtml>

Frutas RAT used in targeted attacks against high-profile companies in Asia and Europe.

Researchers at Symantec identified a cybercriminal campaign targeting high-profile Asian and European organizations in the mining, finance, telecoms, and government sectors that utilizes the Frutas remote access trojan (RAT) to collect information for future targeted attacks. Source: <http://news.softpedia.com/news/Frutas-RAT-Used-in-Targeted-Attacks-Against-High-Profile-Companies-in-Asia-and-Europe-375589.shtml>

Hackers abuse Google Cloud Messaging service in Android malware attacks. Researchers at Kaspersky found that cybercriminals are using a loophole in Google Cloud Messaging to use the service as a command and control server for their Android malware. Source: <http://news.softpedia.com/news/Hackers-Abuse-Google-Cloud-Messaging-Service-to-Distribute-Android-Malware-375327.shtml>

Revealed: Simple 'open sesame' to unlock your HOME by radiowave. Researchers identified a vulnerability in the Z-Wave home-automation standard that allowed them to unlock doors and disable sensors controlled by the technology through a flaw in the implementation of the commands sent to the lock from the encrypted network controller using AES128. Source: http://www.theregister.co.uk/2013/08/13/wave_goodbye_to_security_with_zwave/

Security firm warns of Joomla exploit, users advised to update their installations. Researchers from Verasafe warned users of a zero-day attack in the wild that can control Joomla Web sites and advised them to update their installations. Servers become compromised after users are redirected to a Blackhole landing page and become infected with a Zbot variant. Source: <http://news.softpedia.com/news/Security-Firm-Warns-of-Joomla-Exploit-Users-Advised-to-Update-Their-Installations-375148.shtml>

Bitcoin wallets on Android at risk of theft, developers say. Bitcoin developers announced Bitcoin wallets on Android operating systems are vulnerable to theft after discovering the Android implementation of the Java SecureRandom class contains a number of serious weaknesses. Users were recommended to generate a new address with a repaired random

UNCLASSIFIED

UNCLASSIFIED

number generator and send all the money in the wallet back to themselves. Source: [http://www.computerworld.com/s/article/9241571/Bitcoin wallets on Android at risk of theft developers say](http://www.computerworld.com/s/article/9241571/Bitcoin_wallets_on_Android_at_risk_of_theft_developers_say)

NATIONAL MONUMENTS AND ICONS

(Idaho) **Elk Fire Complex near Pine now nation's no. 1 priority wildfire.** Firefighters reached 5 percent containment August 11 of the Elk Fire Complex after burning over 90,250 acres near Pine. Hundreds of homes were evacuated and an unknown number of others consumed by the fire. Source: http://magicvalley.com/news/local/elk-fire-complex-near-pine-now-nation-s-no-1-priority/article_bca85a32-030d-11e3-9b61-001a4bcf887a.html

POSTAL AND SHIPPING

Nothing Significant to Report

PUBLIC HEALTH

At \$1.2M, photocopy breach proves costly. New York-based Affinity Health Plan settled with the U.S. Department of Health and Human Services for \$1,215,780 after a photocopier containing patient information was compromised. A 2010 investigation uncovered Affinity Health Plan failed to incorporate the electronic protected health information stored on photocopier hard drives after nearly 344,579 individuals were potentially impacted when the company leased a photocopier, stored confidential medical information on its hard drive, and failed to erase the data after returning it. Source: <http://www.healthcareitnews.com/news/12m-photocopy-breach-proves-costly>

TRANSPORTATION

NHTSA servers back online after attack. The National Highway Traffic Safety Administration restored their servers August 12 after 10 of their servers were hacked August 6 which knocked their Web site offline. The documents on the hacked servers were publicly available information and no personal or confidential business information was leaked. Source: <https://threatpost.com/nhtsa-servers-back-online-after-attack/101984>

WATER AND DAMS

Nothing Significant to Report

UNCLASSIFIED

UNCLASSIFIED

HOMELAND SECURITY CONTACTS

To report a homeland security incident, please contact your local law enforcement agency or one of these agencies: **North Dakota State and Local Intelligence Center: 866-885-8295(IN ND ONLY); Email: ndslic@nd.gov; Fax: 701-328-8175 State Radio: 800-472-2121; Bureau of Criminal Investigation (BCI): 701-328-5500; North Dakota Highway Patrol: 701-328-2455; US Attorney's Office Intel Analyst: 701-297-7400; Bismarck FBI: 701-223-4875; Fargo FBI: 701-232-7241.**

To contribute to this summary or if you have questions or comments, please contact:

Kirk Hagel, ND Division of Homeland Security kihagel@nd.gov, 701-328-8168

UNCLASSIFIED